Notice of Allowability	Application No.	Applicant(s)	
	09/592,841	JASON, JR., JAMES L.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Examiner's amendment given on 10/28/05*.

2. ☒ The allowed claim(s) is/are *1-4,6-18,20,21,23-27 and 30*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____.
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Aslam Jaffery and Charles Grey on 10/28/05.

The application has been amended as follows:

1. (Currently Amended) A method for preventing packet retransmissions during Internet Protocol (IP) security (IPsec) security association establishment comprising:

monitoring application socket requests;

requesting a Transmission Control Protocol (TCP) connection by an application;

determining if there is an active IPsec security association that exists to protect network flow associated with the connection request;

preventing the connection request from proceeding to the Transmission Control Protocol of the TCP/IP ~~layer~~ stack if no active IPsec security association exists to protect the network flow;

determining if an IPsec security policy exists for the network flow if no active IPsec security association exists to protect the network flow;

alerting a security association negotiation component to initiate negotiation for the IPsec security association based on the IPsec security policy if the IPsec security policy exists for the network flow; and

allowing the connection request to proceed to the Transmission Control Protocol ~~if one of the active IPsec security associations exist and~~ after the IPsec security association is established from the negotiation.

3. (Currently Amended) The method of claim 1, wherein the IPsec security association is based on one or more of: a source ~~Internet Protocol~~ IP address, a destination IP address, a protocol, a source port, and a destination port.

8. (Currently Amended) The method of claim 7, wherein the network flow information comprises one or more of: a source ~~Internet Protocol (IP)~~ IP address, a destination IP address, a protocol, a source port, and a destination port.

10. (Currently Amended) A method for preventing packet retransmissions during Internet Protocol (IP) security (IPsec) security association establishment comprising:

monitoring application socket requests;

requesting transmission of data on a User Datagram Protocol socket by an application;

determining if the socket has been associated with an active IPsec security association;

determining if there is a defined IPsec security association that may be used to protect network flow if the socket has not been associated with an active IPsec security association;

determining what IPsec security policy should be used when negotiating an IPsec security association for the network flow if there is no defined IPsec security association that may be used to protect the network flow;

preventing the data from being sent to the User Datagram Protocol of the ~~TCP/IP~~

~~layer~~ Transmission Control Protocol (TCP)/IP stack if there is no defined IPsec security association that may be used to protect the network flow;

alerting a security association negotiation component to initiate negotiation for the IPsec security association if there is no defined IPsec security association that may be used to protect the network flow;

establishing the IPsec security association; and

allowing the data to be sent in response to establishment of the IPsec security association.

13. (Currently Amended) The method of claim 10, wherein the second determining comprises comparing filters with one or more of: a source ~~Internet Protocol (IP)~~ IP address, a destination IP address, a protocol, a source port, and a destination port, wherein the destination port includes one or more of a source ~~Internet Protocol (IP)~~ IP address, a destination IP address, a protocol, a source port, and a destination port related to the network flow.

17. (Currently Amended) A system comprising:

~~a network;~~

a network interceptor between ~~the~~ an application ~~layer~~ and the Transmission Control Protocol (TCP) of the ~~TCP/IP layer~~ TCP/Internet Protocol (IP) stack ~~coupled with the network~~, the network interceptor to monitor a TCP connection request by the application ~~an application's socket request~~;

a security association database coupled to the network interceptor, the security association database containing a mapping of network flow information to ~~Internet Protocol~~ IP security (IPsec) security association information;

a security policy database coupled to the network interceptor, the security policy database containing policies that describe parameters that are to be used in a negotiation of an IPsec security association;

a security association negotiation component coupled with the network interceptor, the security association negotiation component to negotiate an IPsec security association to protect network flow associated with the TCP connection request and to establish the IPsec security association;

the network interceptor to allow the TCP connection request to proceed to the Transmission Control Protocol after the IPsec security association is established; and

an ~~(IPsec)~~ IPsec packet classifier, the IPsec packet classifier responsible for performing IPsec processing on incoming and outgoing packets, wherein the network interceptor insures that an IPsec security association is in place before allowing network traffic to flow between the application and the Transmission Control Protocol ~~TCP/IP layer~~.

18. (Currently Amended) The system of claim 17, wherein the network flow information comprises one or more of: ~~Internet Protocol (IP)~~ IP addresses, a protocol, and ports.

20. (Currently Amended) A machine-readable medium having stored thereon data representing sets of instructions which, when executed by a machine, cause the machine to:

monitor application socket requests;

request a Transmission Control Protocol (TCP) connection by an application;

determine if there is an active Internet Protocol (IP) security (IPsec) security association that exists to protect network flow associated with the connection request;

prevent the connection request from proceeding to the Transmission Control Protocol of the TCP/IP ~~layer~~ stack if no active IPsec security association exists to protect the network flow;

determine if an IPsec security policy exists for the network flow if no active IPsec security association exists to protect the network flow;

alert a security association negotiation component to initiate negotiation for an IPsec security association based on the IPsec security policy if the IPsec security policy exists for the network flow; and

allow the connection request to proceed to the Transmission Control Protocol ~~if one of the active IPsec security associations exist and~~after the IPsec security association is established from the negotiation.

23. (Currently Amended) The machine-readable medium of claim 20, wherein the active IPsec security association comprises one or more of: a source ~~Internet Protocol (IP)~~IP, a destination IP, a protocol, a source port, and a destination port.

24. (Currently Amended) A machine-readable medium having stored thereon data representing sets of instructions which, when executed by a machine, cause the machine to:

monitor application socket requests;

request transmission of data on a User Datagram Protocol (UDP) socket by the application;

determine if the socket has been associated with an active Internet Protocol (IP) security (IPsec) ~~IPsec~~ security association;

determine if there is a defined IPsec security association that may be used to protect network flow if the socket has not been associated with an active IPsec security association;

determine what IPsec security policy should be used when negotiating an IPsec security association for the network flow if there is no defined IPsec security association that may be used to protect the network flow;

prevent the data from being sent to the User Datagram Protocol of the Transmission Control Protocol (TCP)/IP ~~TCP/IP layer~~ stack if there is no defined IPsec security association that may be used to protect the network flow;

alert a security association negotiation component to initiate negotiation for the IPsec security association if there is no defined IPsec security association that may be used to protect the network flow;

establish the IPsec security association; and

allow the data to be sent in response to establishment of the IPsec security association.

26. (Currently Amended) The machine-readable medium of claim 24, ~~further cause the machine to negotiate~~ wherein the security association negotiation component negotiates for the IPsec security association using IPsec security parameters specified by an IPsec security policy.

27. (Currently Amended) The machine-readable medium of claim 24, wherein the active IPsec security association comprises one or more of: a source ~~Internet Protocol (IP)~~IP, a destination IP, a protocol, a source port, and a destination port.

30. (Currently Amended) The system of claim 17, ~~wherein the IPsec security association comprises~~ further comprising an Internet Key Exchange (IKE) component.

2. The following is an examiner's statement of reasons for allowance. The present invention is directed to a method and system for securing communications across a network using IP Security. More specifically, independent claims 1, 17 and 20 identify the uniquely distinct features: requesting a TCP connection request by an application,

determining if there is an active IPSec security association that exists to protect the network flow associated with the TCP connection request, and negotiating for an IPSec security association based on a policy if no active IPSec security association exists, the determining and negotiating steps are done before the connection request can proceed to the Transmission Control Protocol of the TCP/IP stack. Independent claims 10 and 24 are similar to claim 1, 17 and 20 in terms of controlling the data flow from the application; the difference is that claims 10 and 24 deal with a UDP transmission request. The closest prior art, Attwood et al. (6,347,376), teaches searching for an IPSec security association either at the TCP or UDP layer as opposed to searching at the IP layer in conventional art. However, Artwood does not disclose searching for an IPSec security association above the TCP or UDP layer. The prior art, taken either singly or in combination, fails to anticipate or fairly suggest the limitations of applicant's independent claim, in such a manner that a rejection under 35 U.S.C 102 or 103 would be proper. The claimed invention is therefore considered to be in condition for allowance as being novel and nonobvious over prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
10/28/05

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100